УДК 004.8+172.4
EDN YVTRVU
DOI: http://dx.doi.org/10.15211/vestnikieran420221829

СТРАТЕГИИ РЕАГИРОВАНИЯ РОССИИ И ЕВРОСОЮЗА НА ГЛОБАЛЬНЫЕ ТЕХНОЛОГИЧЕСКИЕ РИСКИ

Екатерина Дмитриевна Сорокова

МГИМО МИД России, Москва, Россия,
e-mail: sorokova.e.d@my.mgimo.ru, ORCID: 0000-0002-4542-7767

Ссылка для цитирования: Сорокова Е.Д. Стратегии реагирования России и Евросоюза на глобальные технологические риски // Научно-аналитический вестник ИЕ РАН. 2022. №4. С. 18-29. DOI: 10.15211/vestnikieran420221829

Аннотация. *В статье на материале докладов Всемирного экономического форума (2006–2022 гг.) даётся определение глобальных рисков современности, выделяется перечень групп наиболее актуальных технологических рисков. Обозначается их политическое измерение. Проводится сравнение мер реагирования России и Евросоюза на два наиболее актуальных риска: «неблагоприятные последствия развития технологий» и «концентрация цифровой мощи». Показано, что Россия и ЕС в целом прибегают к схожим стратегиям и мерам реагирования. На фоне нарастания конкуренции между различными технико-экономическими моделями и усиления транснациональных цифровых корпораций РФ и ЕС стремятся укрепить цифровой суверенитет: предпринимают меры по усилению законодательного регулирования деятельности «ИТ-гигантов», поддержке собственной конкурентоспособности, развитию технологий и инфраструктурной устойчивости, защите персональных данных граждан. Кроме того, и Россия, и ЕС постепенно выстраивают комплексную систему реагирования для предотвращения неприемлемых социо-гуманитарных последствий цифровой трансформации. Она включает в себя как подготовку нормативно-правовой базы и совершенствование концептуальных подходов, так и «мягкие» способы регулирования (разработку этических требований).*

Ключевые слова: *глобальные технологические риски, Россия, Европейский союз, реагирование, управление рисками, искусственный интеллект.*

Статья поступила в редакцию: 10.08.2022.

THE STRATEGIES OF POLICY RESPONSE TO GLOBAL TECHNOLOGICAL RISKS: THE CASES OF RUSSIA AND THE EU

Ekaterina D. Sorokova

MGIMO University, Moscow, Russia,
e-mail: sorokova.e.d@my.mgimo.ru, ORCID: 0000-0002-4542-7767

For citing: Sorokova, E.D. (2022). The strategies of policy response to global technological risks: the cases of Russia and the EU. Nauchno-analiticheskij vestnik IE RAN 28(4): 18-29. (in Russian). DOI: 10.15211/vestnikieran420221829

Abstract*. The article explores the concept of global technological risks and attempts to define their political dimension. The author analyses the «Global Risks Reports» of the World Economic Forum published over the last 16 years, identifies four groups of risks repeatedly highlighted by experts. Based on the results of this research, the author compares the policy response strategies of Russia and the EU to two most recent risks, namely «Adverse outcomes of technological advances» and «Digital power concentration». The results show that Russia and the EU generally resort to similar measures in their policy response strategies. Increasing competition between the technical and economic models of the United States and China and the rise of digital corporations prompt Russia and the EU to strengthen their digital sovereignty. Most notably, both actors develop stricter legislative regulation to contain the activities of «IT giants», as well as foster their own competitiveness, technology development, infrastructural stability and personal data protection rules. Additionally, both Russia and the EU are gradually building a policy response system to prevent unacceptable humanitarian consequences of digital transformation. They combine the development of regulatory frameworks and conceptual approaches with «soft law», such as ethical requirements.*
Key words*: global technological risks, Russia, European Union, policy response, risk management, artificial intelligence.*

Article received: 10.08.2022.

В эпоху глобализации и грядущей четвёртой промышленной революции особенно актуальными стали концептуализация и разработка комплексных стратегий реагирования на непредсказуемые последствия развития и внедрения новейших технологий, а также риски, связанные с бесконтрольным наращиванием и использованием технологического потенциала различными акторами. В этих условиях как Российская Федерация, так и Европейский союз заинтересованы в минимизации рисков – не только военных, но и социально-гуманитарных, связанных с интенсивным развитием цифровизации; в обеспечении собственной безопасности и цифрового суверенитета, сохранении траектории общественного развития.

Тенденция к возрастанию внимания к технологическим рискам и разработке политических инструментов реагирования на них прослеживается в том числе в докладах крупнейшей международной экспертной площадки – Всемирного экономического форума в Давосе (далее – ВЭФ). С опорой на доклады ВЭФ 2006–2022 гг. выделены перечень и ключевые характеристики наиболее значимых из них. Исходя из этого, проанализированы стратегии реагирования России и Евросоюза на два наиболее актуальных глобальных технологических риска – внешний (концентрация цифровой мощи) и внутренний (неблагоприятные последствия технологического прогресса).

Глобальные технологические риски и их политическое измерение

Современное изучение рисков прошло долгий путь от математизированного, формализованного подхода в сторону гуманитаризации, междисциплинарности и учёта контекстов их генерации, восприятия и распространения последствий (в т.ч. социо-экономических, антропологических и др.). Технологические и техногенные риски традиционно находились в фокусе

исследователей (например, крупнейших представителей социологического подхода – У. Бека и Э. Гидденса).

Глобализация рисков на рубеже XX–XXI вв. поставила под вопрос онтологическую безопасность человека. В отличие от эпохи модерна, они обрели качественно новые характеристики – *делокализацию* (неограниченность причин и последствий в пространстве, времени и общественных взаимосвязях), *некалькулируемость* (невозможность просчитать последствия) и *некомпенсируемость* (невозможность полного восстановления системы после перенесённого шока и необратимость последствий) (термины У. Бека) (Ломако 2018: 268).

Стоит выделить политическое измерение глобальных рисков и характера реагирования на них. Отличие двух стратегий – управления рисками и формирования стрессоустойчивости системы, по замечанию эксперта Центра инженерных исследований и разработок армии США (*ERDC*) И. Линькова, состоит в комплексном вѝдении. Если первая предполагает работу с отдельно взятым элементом системы, то проектирование стрессоустойчивости нацелено на определение функциональных возможностей системы, наиболее важных для всех участников, и разработку социально-технологических методов и решений для поддержания их устойчивости в условиях широкого спектра угроз (Linkov 2014: 408).

Реформирование системы реагирования на риски требует концептуальных перемен, принятия стратегических решений, выстраивания системы взаимодействия с различными заинтересованными сторонами. Основная ответственность за них ложится на государство как главного гаранта безопасности граждан. Именно от него ожидают комплексной оценки и прогнозирования социо-гуманитарных последствий политики цифровизации, интенсивного развития и внедрения новых технологий.

Таким образом, современные реалии и подходы требуют рассмотрения глобальных рисков в неразрывной связи с реагированием на них. Концептуальное оформление и адаптация системы к новым условиям не сводится исключительно к вопросам менеджмента, а предполагает изменения в стратегических подходах к рискам, что требует проявления политической воли руководства страны.

За 16 лет публикации докладов ВЭФ, во многом ориентированных на лиц, принимающих решения в бизнесе и политике, толкование глобальных рисков претерпело примечательные изменения. Полезно их проследить. На самых первых этапах для определения глобального риска выделялось только три аспекта: взаимозависимость, эвристические предубеждения и ошибки в политике (стоит отметить, что два из трёх признаков связаны непосредственно с действиями акторов, призванными снизить риск) (Global Risks Report 2007: 19-20). В последующих выпусках набор характеристик, применявшихся для описания термина, расширился: «чтобы *угроза* считалась *глобальным риском*, она должна иметь глобальный географический охват, межотраслевую значимость, неопределённость времени возникновения и проявлений, высокий уровень экономического и/или социального воздействия, и требовать многостороннего подхода к реагированию…» (Global Risks Report 2011: 44). В 2014 г. глобальный риск вполне чётко определялся как «*событие*, которое оказывает значительное негативное воздействие...», при этом его главным качеством считался потенциально *системный характер* (возможное наступление сбоев во всей системе, а не только в отдельных её частях или компонентах) (Global Risks Report 2014: 12). С 2015 г. и вплоть до 2021 г. глобальным риском уже называлось «*неопределённое событие* или *состояние*…» (Global Risks Report 2015: 56). В докладе 2022 г. речь идёт о «*возможности события* или *состояния*, могущих вызвать значительные негативные последствия для нескольких стран или отраслей… в следующие 10 лет» (Glo-

bal Risks Report 2022: 93)[1].

Примечательно, что определение изменилось в сторону большей аморфности риска как фено́мена: из «угрозы» (2011 г.) он трансформировался в более нейтральное «событие» с негативными последствиями, потом – в «неопределённое событие или состояние», а позже – в «возможность наступления события или состояния». Таким образом, в эволюции формулировки просматривается снижение предсказуемости и прогнозируемости глобальных рисков. Отметим, что фактически выделенные экспертами ВЭФ признаки конкретизируют три параметра У. Бека – делокализацию, некалькулируемость и некомпенсируемость.

С 2006 г. глобальные технологические риски (далее – ГТР) в рамках классификации ВЭФ выделяются в качестве самостоятельной группы. Формулировки отдельных рисков, как и их номенклатура в целом, значительно изменились, но анализ перечней ГТР позволяет определить четыре ведущих, «сквозных» риска, неизменно отмечавшихся экспертами. Среди них: нарушение критической (информационной) инфраструктуры; защита данных; угрозы, связанные с новыми технологиями (здесь можно выделить две подгруппы – их непредсказуемые последствия и уязвимость информационного пространства). В отдельную, четвёртую, категорию автором выделены «новейшие риски», введённые в перечень в 2021 г. и оставшиеся в нём в докладе 2022 г.: «концентрация цифровой мощи» (*digital power concentration*) и «цифровое неравенство».

Интересно рассмотреть подробнее стратегии реагирования России и Евросоюза на два ГТР из двух последних групп, квалифицированных экспертами сравнительно недавно: «концентрация цифровой мощи» и «неблагоприятные последствия технологического прогресса».

Концентрация цифровой мощи

Данную категорию, впервые введённую в перечень в качестве самостоятельного риска в 2021 г., эксперты ВЭФ определяют как «концентрацию критически важных цифровых активов, возможностей и/или знаний у ограниченного числа частных лиц, предприятий или государств, что приводит к механизмам ценообразования по собственному усмотрению, отсутствию беспристрастного надзора, неравному доступу частных лиц и/или общества …» (Global Risks Report 2022: 95).

О. Ребро, эксперт Института международных исследований МГИМО, отмечает проявившееся в 2020-х гг. пробуждение национального цифрового самосознания, происходящее параллельно с определением государствами своей роли в новых условиях, заданных технологической революцией. Уже сейчас намечаются различия в национальных подходах к определению принципов функционирования цифрового пространства и готовность стран отстаивать своё право на независимое определение этих принципов (Ребро 2022: 61). И Россия, и Евросоюз серьёзно подходят к вопросу обеспечения цифрового суверенитета на фоне нарастания конкуренции технико-экономических моделей, продвигаемых, в частности, США и Китаем (Безруков 2021: 10-11). Несмотря на то что это понятие прочно вошло в политический дискурс, единое определение так и не выработано. При этом такие элементы, как независимость научных разработок, установление стандартов, безопасность инфраструктуры связи относятся к более широкому понятию «технологического суверенитета», равно применимому и к «доцифровой» эпохе (Ребро 2022: 50).

Рост опасений, связанных с технологическим усилением соседних государств, и возникающую на их почве «гонку технологий» можно считать частным случаем «дилеммы безопасности» (Jervis 1978). О рисках технологических гонок, могущих привести к катастрофи-

[1] Курсив авторский – Е.С.

ческим последствиям, подробно писал Н. Бостром в статье «Гонка к пропасти» (Armstrong 2013). Однако соперничество стран в технологической сфере и стремление предотвратить установление господства одной из них само по себе не ново.

В контексте обеспечения странами своего цифрового суверенитета и борьбы с концентрацией цифровой мощи стоит обратить внимание на стратегии их действий в отношении негосударственных акторов – прежде всего, крупных транснациональных корпораций (Google, Apple, Meta, ByteDance и др.), усиление которых в равной степени вызывает беспокойство и России, и ЕС. Государства заинтересованы в снижении зависимости от иностранных компаний и поставщиков цифровых услуг.

Так, и в России, и в ЕС особое внимание уделялось хранению и защите персональных данных, подвергающихся сбору и обработке со стороны транснациональных платформ.

В России в 2015 г. вступил в силу Федеральный закон № 242-ФЗ, который обязал иностранные компании локализовать базы данных россиян на местных серверах в случае, если её деятельность направлена на территорию России и если компания осуществляет сбор персональных данных граждан РФ. В конце 2021 г. вступил в силу Закон о «приземлении» (Федеральный закон № 236-ФЗ). ИТ-компании (и другие иностранные владельцы инфоресурсов) с аудиторией больше 500 тыс. российских пользователей в день были обязаны открыть полномочное представительство в РФ, зарегистрировать личный кабинет на сайте Роскомнадзора и разместить специальную форму для обращений российских граждан и организаций. Эти меры призваны не только обеспечить безопасность данных россиян, но и упорядочить коммуникацию государственных органов и самих граждан с иностранными компаниями; упростить разрешение споров (в т.ч. в судебном порядке) и вопросов, связанных с модерацией контента: судебные органы и регулятор не раз сталкивались с тем, что российские офисы многих ИТ-гигантов (например, ООО «Гугл») не обладали полномочиями по модерации, поскольку являлись лишь рекламными или маркетинговыми подразделениями компаний (Офис Google в… 2020).

Строгий и комплексный подход к регулированию ИТ-гигантов реализуется в ЕС. В 2018 г. вступил в силу Общий Регламент по защите данных (*GDPR*), реализация которого стала вехой на пути укрепления безопасности данных и защиты личной информации в рамках Единого цифрового рынка ЕС.

В 2022 г., вероятно, будет окончательно реформировано законодательство об онлайн-торговле, которое принципиально не менялось почти 20 лет с момента принятия Директивы по электронной торговле и дополняющих её нормативных актов в 2000–2002 гг. (*E-commerce directive*). Закон о цифровых услугах (*Digital Services Act, DSA*) и Закон о цифровых рынках (*Digital Markets Act, DMA*) строго регламентируют бизнес- и рекламную деятельность работающих в ЕС крупнейших платформ (*gatekeepers*) и призваны установить новый всеобъемлющий набор правил для цифровых сервисов.

В апреле 2022 г. по законопроекту о цифровых услугах было достигнуто политическое соглашение между Европарламентом и Еврокомиссией. Согласно *DSA*, компании будут обязаны не только иметь в ЕС представителя, уполномоченного на контакты с государственными органами, но и раскрывать информацию о правилах показа рекламы, удалять противоправный и иной вредоносный контент, ограничить использование «тёмных паттернов» алгоритмов, самостоятельно оценивать риски и принимать меры по их снижению, проводить независимые проверки прозрачности «рекомендательных сервисов». В случае принятия закона «крупнейшие онлайн-игроки» (платформы и поисковые системы) будут обязаны соблюдать нормы *DSA* уже спустя четыре месяца после признания их таковыми, в то время как в отношении

остальных акторов документ будет напрямую применяться через 15 месяцев после вступления в силу (Auestions and Answers: Digital… 2022). Это наглядно демонстрирует приоритеты ЕС по установлению «правил игры» для влиятельных игроков.

В свою очередь, *DMA* фактически направлен на то, чтобы повысить подотчётность крупнейших платформ и предотвратить нарушения правил конкуренции: предпочтение собственным сервисам, «выдавливание» альтернативных производителей с платформы, воспрепятствование доступу бизнесменов к конечным пользователям. Его исполнение будет контролироваться Еврокомиссией. При этом за нарушение правил предполагается возможность штрафа в размере до 10% глобального оборота компании, за повторное нарушение – до 20% (Digital Markets Act: Commission… 2022).

Однако помимо создания таких «правил игры», предотвращение концентрации цифровых ресурсов предполагает поддержку собственной конкурентоспособности, развитие технологической отрасли и инфраструктурной устойчивости. И в России, и в ЕС это рассматривают как стратегическую задачу.

В 2019 г. был принят закон (Федеральный закон №90-ФЗ от 01.05.2019 г.), призванный обеспечить устойчивое, безопасное и целостное функционирование российского сегмента Интернета даже в случае невозможности подключения к зарубежным корневым серверам или злонамеренного внешнего воздействия. Его реализация предполагает регулярное проведение учений органов власти, операторов связи и владельцев технологических сетей по выявлению угроз и восстановлению работоспособности российского сегмента сети Интернет. Законом предусмотрена и возможность минимизировать передачу за рубеж данных, которыми обмениваются российские пользователи (Подписан закон, направленный… 2019).

В Евросоюзе также обеспокоены безопасностью инфраструктуры облачных сервисов. В 2019 г. Франция и Германия инициировали проект *Gaia X*, объединивший более 300 компаний. Он предполагает создание рассредоточенной и не зависимой от иностранных (прежде всего американских) производителей и поставщиков услуг «облачной» инфраструктуры (What is Gaia-X… 2022).

Приоритетные направления цифровой трансформации Евросоюза были обозначены в сообщении Еврокомиссии «Цифровой компас – 2030: европейский путь в цифровое десятилетие». Документ конкретизировал положения цифровой стратегии ЕС, опубликованной в 2020 г., и приоритеты, обозначенные в выступлении председателя ЕК У. фон дер Ляйен: обеспечение цифрового суверенитета объединённой Европы, формирование общего ви́дения укрепления цифрового лидерства ЕС к 2030 г. и обозначение его целей и принципов. «Цифровой компас» определил четыре направления цифровой трансформации: улучшение цифровых навыков граждан и повышение уровня профессиональной подготовки специалистов в цифровой сфере; безопасная, высокопроизводительная и устойчивая цифровая инфраструктура; цифровая трансформация бизнеса и цифровизация государственных услуг (2030 Digital Compass…: 1; 4-9).

В России Указом Президента РФ от 21 июля 2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года» также были определены четыре показателя для достижения национальной цели «цифровой трансформации». В их числе: достижение «цифровой зрелости» ключевых отраслей экономики и социальной сферы (включая здравоохранение, образование и государственное управление); увеличение доли массовых социально значимых услуг, доступных в электронном виде, до 95%; рост доли домохозяйств, обеспеченных возможностью широкополосного доступа к Интернету, до 97%; увеличение вложений в отечественные решения в сфере информационных технологий в четыре раза по сравне-

нию с показателем 2019 г. Стоит отметить социальную направленность большинства целей и внимание, уделённое здравоохранению и образованию (Указ Президента Российской Федерации… 2020).

Неблагоприятные последствия технологического прогресса

Перечень новейших технологий, пользование которыми может потенциально привести к масштабным неблагоприятным последствиям, неоднократно расширялся экспертами ВЭФ. История этой категории началась с единственного пункта «Нанотехнологии» в 2006 г. Серьёзная трансформация произошла в 2011–2012 гг., когда обобщённая формулировка «угрозы, исходящие от новых технологий» (Global Risks Report 2011: 47) была разделена на восемь подпунктов. В 2016 г. длинная формулировка «Массовое и широкомасштабное злоупотребление технологиями (3D-печать, искусственный интеллект, геоинженерия, синтетическая биология и т.д.)» (Global Risks Report 2015: 4) стала более ёмкой: «Неблагоприятные последствия развития технологий» (Global Risks Report 2016: 5), и сохранилась в таком виде до 2022 г. с незначительным изменением: «Неблагоприятные результаты развития технологий» (Global Risks Report 2022: 95).

При рассмотрении реагирования на новейшие технологии особенно интересен подход к искусственному интеллекту (ИИ). ЕС декларирует намерение стать лидером в сфере этичного и «вызывающего доверие ИИ». В 2018–2019 гг. он был объявлен одним из стратегических приоритетов экономической и научно-технической политики ЕС в сообщении Еврокомиссии «Об ИИ для Европы». Россия также намерена занять достойное место в ряду международных лидеров. Указом Президента РФ № 490 от 10 октября 2019 г. была утверждена Национальная стратегия в сфере развития ИИ.

При этом и в России, и в ЕС обеспокоены возможными социо-экономическими последствиями широкого и интенсивного внедрения технологий ИИ во все сферы жизни общества, включая «чувствительные» для безопасности – сфера образования, здравоохранения, найма, кредитования, государственных услуг и т.д. На первый взгляд, логично купировать столь непредсказуемый тип риска с помощью законодательных ограничений. Однако законодатели стараются проявить больше гибкости, чтобы использовать возможности технологического прогресса.

Попытки практически воплотить такую стратегию можно наблюдать как в России, так и в ЕС. Оба актора заявляют, что в основе регулирования в сфере ИИ лежит риск-ориентированный подход. Но уже сейчас можно наблюдать усложнение концептуального представления как о самом фено́мене ИИ, так и о его регулировании.

Какие же риски и модели реагирования на них описываются в существующих инициативах и документах России и ЕС?

В 2018–2021 гг. в ЕС с привлечением научного сообщества активно разрабатывались «мягкие» этические нормы разработки и внедрения ИИ. В 2021 г. Еврокомиссия представила проект «Акта об ИИ», где была предложена модель реагирования, предполагающая контроль за соответствием технологий ИИ нормам и стандартам до и после выхода на рынок Евросоюза.

В законопроекте представлена классификация систем ИИ по степени риска и выделена особая категория систем с неприемлемым уровнем риска, на которую предлагается наложить запрет. Примечательно, что они связаны с информационно-психологической безопасностью и нарушением прав человека: манипуляциями психикой и поведением человека, эксплуатацией уязвимых сторон, составлением социального рейтинга. Высокорискóвыми считаются си-

стемы, затрагивающие здоровье, безопасность и основные права человека, а также используемые в образовании, сфере услуг, при решении вопросов миграции и предоставления убежища и пр. Они подлежат жёсткому контролю до и после выхода на рынок ЕС. Системы с низким риском (чат-боты и др.) предлагается оставить на уровне саморегулирования отдельных организаций и отраслей (Proposal for a Regulation, 2022).

В правово́м регулировании ЕС делается акцент на вопросе ответственности за действия систем ИИ, которые не наделены правосубъектностью. Для лиц, осуществляющих эксплуатацию высокорискóвых систем ИИ, предусмотрен режим строгой ответственности, для эксплуатантов систем с меньшим риском – ответственность, основанная на виновности (Марченко 2021a: 137).

Серьёзным этапом в продвижении отечественного регулирования ИИ стало создание в 2021 г. российского Кодекса этики в сфере ИИ, где были закреплены её общие принципы и механизм их реализации через институты уполномоченных и комиссий по этике, создаваемых в организациях-подписантах. Российский подход утверждает защиту интересов и прав людей и отдельного человека как приоритет развития ИИ; принцип ответственности за создание и использование ИИ и закрепление её за человеком (а не машиной); применение ИИ по назначению и на благо человека; приоритет развития технологий над интересами конкуренции; прозрачность и правдивость информирования о возможностях и рисках систем ИИ (Кодекс этики в сфере… 2021).

Кроме того, в конце 2021 г. был представлен проект «закона о роботах», где предложена система регулирования оборота роботов на территории России, а также классификация автономных устройств по видам (гражданские и служебные, управляемые и автономные) и степени опасности, предусмотрен контроль за тремя классами из четырёх выделенных. Было в нём и предложение запретить роботов, которые могут использоваться в качестве оружия или в преступных целях, отдельно был подчёркнут запрет на таких роботов, способных к автономному принятию решений (В Совфеде разработали… 2021). Хотя перспективы законопроекта остаются неясными, он показателен как проявление тенденции к созданию комплексной системы регулирования взаимодействия человека и машины, дифференциации подхода к технологиям ИИ, представляющим различную степень риска.

Примечательно, что в ЕС и России наблюдается постепенный отход от антропоморфного восприятия ИИ, придающего ему человеческие качества, и отказ от наделения систем ИИ правосубъектностью. Так, в Акте ЕС об ИИ даётся определение понятия «система ИИ» как «программного обеспечения, …способного для заданного человеком набора целей производить выходные данные, такие как контент, прогнозы, рекомендации или решения, влияющие на среду, с которой они взаимодействуют». В этой трактовке наблюдается отход от определения ИИ через проведение аналогии с интеллектом, способностями и разумными действиями человека (Марченко 2021b: 33), которая прослеживалась в более раннем, ориентировочном варианте определения в сообщении Еврокомиссии «Об ИИ для Европы» 2018 г., где под ИИ понимались «системы, которые демонстрируют разумное поведение, анализируя окружающую среду и предпринимая действия – с некоторой степенью автономии – для достижения конкретных целей» (Communication… 2018: 1). В России официальное определение ИИ (2019 г.) остаётся построенным на сравнении с человеческими достижениями: это «комплекс технологических решений, позволяющий имитировать когнитивные функции человека… и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека» (Указ Президента Российской Федерации… 2019: 5, пункт а). Однако уже в Кодексе (2021 г.) подчёркивается необходимость со-

блюдения границ и разумной дистанции между человеком и машиной, сохранения автономии человека и его контроля над ИИ, предотвращения деструктивного влияния ИИ на когнитивные функции человека и сферу его духовно-нравственного развития, недопустимость наделения ИИ правосубъектностью.

* * *

Современные глобальные риски целесообразно рассматривать в неразрывной связи с реагированием, поскольку глобализация рисков XXI в. поставила под угрозу безопасность на всех уровнях и потребовала выстраивания более сложных и комплексных подходов к реагированию.

Определение понятия «глобальные риски» в докладах ВЭФ претерпело изменения в сторону увеличения неопределённости, характеризующей как само это явление, так и его возникновение: конкретное обозначение «угроза» трансформировалось в более мягкое «событие» с негативными последствиями, позже – в «*неопределённое* событие или состояние», и к 2022 г. – в «*возможность наступления* события или состояния».

В аналитических докладах ВЭФ 2006–2022 гг. были выделены четыре «сквозных» глобальных технологических риска: нарушение критической информационной инфраструктуры; защита данных; угрозы, связанные с новыми технологиями, и «новейшие» – «концентрация цифровой мощи» и «цифровое неравенство». В статье рассмотрены стратегии реагирования РФ и ЕС на два риска из четырёх перечисленных групп – «концентрацию цифровой мощи» и «неблагоприятные последствия технологического прогресса».

И Россия, и Евросоюз в целом прибегают к схожим стратегиям реагирования на рассматриваемые риски: проводят последовательную политику по укреплению собственного цифрового суверенитета и выстраиванию комплексной системы реагирования для предотвращения неприемлемых социо-гуманитарных последствий цифровой трансформации.

В условиях нарастания конкуренции и усиления цифровых ТНК предпринимаются меры по совершенствованию законодательного регулирования деятельности «техногигантов» как в национальных, так и в общеевропейской юрисдикциях ЕС. Усиливается антимонопольное регулирование, устанавливаются требования по локализации персональных данных пользователей и ограничения на их трансграничную передачу, выдвигаются инициативы по созданию рассредоточенной и не зависящей от иностранных производителей инфраструктуры связи, включая «облачную», и др.

Россия и ЕС стремятся с помощью сочетания законодательных и более мягких способов регулирования предотвратить неприемлемые гуманитарные последствия развития новейших технологий. Например, в случае с ИИ (одним из приоритетов цифровой трансформации), наблюдается постепенный отход от его антропоморфизации и наделения правосубъектностью, ведётся поиск более гибких методов регулирования касательно создания, внедрения и использования ИИ, дифференцируется подход к технологиям ИИ, представляющим различную степень риска.

Список литературы / References

2030 Digital Compass: the European Way for the Digital Decade. European commission. 09.03.2021. Available at: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en (accessed 03.08.2022).

Armstrong, S., Bostrom, N., Shulman, C. (2013). Racing to the precipice: a model of artificial

intelligence development. Technical Report. Future of Humanity Institute; Oxford University.

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions «Artificial Intelligence for Europe». EUR-Lex. 25.04.2018. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0237&from=EN (accessed 03.08.2022).

Digital Markets Act: Commission welcomes political agreement on rules to ensure fair and open digital markets. European commission. 25.03.2022. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1978 (accessed 03.08.2022).

Global Risks Report 2007. World Economic Forum. 01.2007. Available at: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2007.pdf (accessed 03.08.2022).

Global Risks Report 2011. World Economic Forum. 01.2011. Available at: https://reports.weforum.org/wp-content/blogs.dir/1/mp/uploads/pages/files/global-risks-2011.pdf (accessed 03.08.2022).

Global Risks Report 2014. World Economic Forum. 01.2014. Available at: https://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf (accessed 16.08.2022).

Global Risks Report 2015. World Economic Forum. 01.2015. Available at: https://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf (accessed 03.08.2022).

Global Risks Report 2022. World Economic Forum. 11.01.2022. Available at: https://www.weforum.org/reports/global-risks-report-2022/ (accessed: 03.08.2022).

Jervis, R. (1978). Cooperation Under the Security Dilemma. World Politics 2(30): 167-214.

Linkov, I. (2014). Changing the resilience paradigm. Nature climate change (4): 407-409. Available at: https://www.nature.com/articles/nclimate2227 (accessed 02.08.2022).

Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts 2021. EUR-Lex. 21.04.2021. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206 (accessed 03.08.2022).

Questions and Answers: Digital Services Act. European Commission. 20.05.2022. Available at: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348 (accessed 03.08.2022).

What is Gaia-X? Available at: https://www.gaia-x.eu/what-gaia-x/factsheet (accessed 03.08.2022).

Безруков, А.О. (2021). Realpolitik в «цифре»: суверенитет, союзы и неприсоединение XXI века. Валдай. 01.09.2021. [Bezrukov, A.O. (2021). Realpolitik «in the Digital Domain»: Sovereignty, Alliances and Non-Alignment of the XXI Century. Valdai. 01.09.2021. (In Russian)] Available at: https://ru.valdaiclub.com/files/39047/ (accessed 03.08.2022).

В Совфеде разработали законопроект, описывающий взаимоотношения робота и человека в РФ. ТАСС. 20.12.2021. [The Federation Council Has Drafted a Bill Describing the Relationship between a Robot and a Human in the Russian Federation. TASS. 20.12.2021. (In Russian)]. Available at: https://tass.ru/obschestvo/13243537 (accessed 03.08.2022).

Жердина, С. (2017). Локализация персональных данных россиян для иностранных компаний. Юрист (45): [Zherdina, S. (2017). The Localization of Russians' Personal Data for Foreign Companies. Jurist (45). (In Russian)]. Available at: https://www.vegaslex.ru/mobile/analytics/publications/localization_of_personal_data_of_russians_for_foreign_companies/ (accessed 03.08.2022).

Кодекс этики в сфере искусственного интеллекта. Aiethic. 26.10.2021. [A Code of Ethics in the Sphere of Artificial Intelligence. Aiethic. 26.10.2021. (in Russian)]. Available at: https://www.aiethic.ru/code (accessed 03.08.2022).

Ломако, О.М. (2018). Мировое общество риска в политической философии Ульриха Бека // Известия Саратовского университета. Серия: Философия. Психология. Педагогика 3(18):

265-269. [Lomako, O.M. (2018). The World Risk Society in Ulrich Beck's Political Philosophy. Izvestiya of Saratov University. Philosophy. Psychology. Pedagogy 3(18): 265-269. (In Russian)]. DOI: 10.18500/1819-7671-2018-18-3-265-269

Марченко, А.Ю. (2021a). Правовой статус систем искусственного интеллекта и проблема определения ответственности за их действия по праву Европейского союза // Современная наука: актуальные проблемы теории и практики. Серия: Экономика и право (8): 134-138. [Marchenko, A.Yu. (2021a). The Legal Status of Artificial Intelligence Systems and the Problem of Determining Responsibility for their Actions under the Law of the European Union. Modern Science: Actual Problems of Theory and Practice. Series: Economics and Law (8): 134-138. (In Russian)]. DOI: 10.37882/2223-2974.2021.08.19

Марченко, А.Ю. (2021b). Правовое регулирование технологий ИИ в Европейском союзе: текущее состояние и перспективы его развития // Юридическая наука (7): 32-36. [Marchenko, A.Yu. (2021b). Legal Regulation of AI Technologies in the European Union: Current State and Prospects for Development. Legal Science (7): 32-36. (In Russian)].

ООО «Гугл». Rusprofile. [Google LLC. Rusprofile. (In Russian)]. Available at: https://www.rusprofile.ru/okved/1034637 (accessed 03.08.2022).

Офис Google в России уклонился от ответа по поводу блокировки каналов СМИ РФ на YouTube. ТАСС. 13.08.2020. [Google's office in Russia Evaded an Answer Concerning the blocking of Russian Media Channels on YouTube. TASS. 13.08.2020. (In Russian)]. Available at: https://tass-ru.turbopages.org/tass.ru/s/ekonomika/9192533 (accessed 03.08.2022).

Подписан закон, направленный на обеспечение безопасного и устойчивого функционирования интернета на территории России. Президент России. 01.05.2019. [A Law Aimed at Ensuring the Safe and Sustainable Functioning of the Internet in Russia is Signed. The President of Russia. 01.05.2019. (In Russian)]. Available at: http://www.kremlin.ru/acts/news/60430 (accessed 03.08.2022).

Ребро, О.В. (2022). Категория «цифрового суверенитета» в современной мировой политике: вызовы и возможности для России // Международные процессы 4(19): 47-67. [Rebro, O.V. (2022). The Notion of «Digital Sovereignty» in Modern World Politics. Challenges and Opportunities for Russia. International Trends 4(19): 47-67. (In Russian)]. DOI 10.17994/IT.2021.19.4.67.6

Сорокова, Е.Д. (2022). Реагирование России и ЕС на глобальные технологические риски ИИ: социально-политический аспект // XVI Международная научная конференция «Сорокинские чтения – 2022»; Сборник материалов. М.: МАКС Пресс. С. 402-403. [Sorokova, E.D. (2022). The Policy Response of Russia and the EU to Global Technological Risks of AI: a Socio-Political Aspect. In: XVI International Scientific Conference «Sorokin readings – 2022». Collection of materials. Moscow: MAKS Press: 402-403]. DOI: 10.29003/m3033.16sr-2022

Указ Президента Российской Федерации № 490 «О развитии искусственного интеллекта в Российской Федерации». Президент России. 10.10.2019. [Decree of the President of the Russian Federation № 490 «On the Development of Artificial Intelligence in the Russian Federation». The President of Russia. 10.10.2019. (In Russian)]. Available at: http://www.kremlin.ru/acts/bank/44731 (accessed 03.08.2022).

Указ Президента Российской Федерации № 474 «О национальных целях развития Российской Федерации на период до 2030 года». Официальный интернет-портал правовой информации. 21.07.2020. [Decree of the President of the Russian Federation № 474 «On the National Development Goals of the Russian Federation for the period up to 2030». The Official Internet Portal of Legal Information. 21.07.2020. (In Russian)]. Available at: http://publication.pravo.gov.ru/Document/View/0001202007210012?index=2&rangeSize=1 (accessed 03.08.2022).

Федеральный закон № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети “Интернет” на территории Российской Федерации». Consultant.ru. 01.07.2021. [Federal Law № 236-FZ «On the Activities of Foreign Persons in the Information and Telecommunications Network “Internet” on the Territory of the Russian Federation». Consultant.ru. 01.07.2021. (In Russian).] Available at: http://www.consultant.ru/document/cons_doc_LAW_388781/ (accessed 03.08.2022).